THAT WHICH IS CLAIMED IS:

1.   A block cipher device for a cryptographically secured digital communication system comprising:

a pair of first stages connected in parallel and receiving an input data block and a control data block, each first stage defining a respective first data path and comprising

a sum modulo-two unit responsive to the control data block and the input data block, and

a first nibble swap unit downstream from said sum modulo-two unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said sum modulo-two unit;

a diffuser connected in both of the first data paths for mixing data therebetween;

a key scheduler receiving a key data block and generating a random key data block based thereon;

a pair of second stages connected in parallel downstream from said first stages and receiving the random key data block, the control data block and output signals from said first stages, each second stage defining a respective second data path and comprising

a first linear modulo unit responsive to the random key data block, one of the output signals from said first stages, and the control data block for performing a modulo summing operation based on a first modulus q,

an nth power modulo unit responsive to an output signal from said first linear modulo unit for performing an nth power modulo operation based on a second modulus p, and

a second linear modulo unit responsive to the random key data block and an output signal from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r,

each first, second and third modulus q, p and r being unique from each other; and

an output stage connected to said second stages for generating an output data block for the block cipher device.

2.   A block cipher device according to Claim 1 wherein said first and second stages are selectively configurable so that one first data path and one second data path are operational; and said diffuser is bypassed.

3.   A block cipher device according to Claim 1 wherein said diffuser is connected in both of the first data paths between the respective sum modulo-two units and first nibble swap units.

4.   A block cipher device according to Claim 1 wherein each first stage further comprises a substitution/expansion unit downstream from said first nibble swap unit and being responsive to an output signal therefrom for providing customizable cipher variations.

5. A block cipher device according to Claim 4 wherein each first stage further comprises a second nibble swap unit downstream from said substitution/ expansion unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said substitution/expansion unit.

6. A block cipher device according to Claim 1 further comprising a nibble interleave unit connected in both of the first data paths for reordering data therebetween.

7. A block cipher device according to Claim 1 further comprising a substitution unit connected in both of the first data paths for substituting data therebetween.

8. A block cipher device according to Claim 1 wherein each nth power modulo unit provides an output signal of predetermined size, with $n>1$ and with $p=2^K-X$, where X is selected such that a greatest common denominator between n and (2^K-X-1) is 1 and K is the predetermined size.

9. A block cipher device according to Claim 1 wherein said key scheduler comprises a pair of look-up tables for generating the random key data block.

10. A block cipher device according to Claim 9 wherein said key scheduler further comprises a pair of shift registers responsive to the received key data

block; and wherein each look-up table is responsive to a corresponding shift register.

11. A block cipher device according to Claim 10 wherein said key scheduler further comprises a pair of combiners responsive to outputs from said shift registers and to outputs from said look-up tables, each combiner combining the output from a corresponding shift register and the output from a corresponding look-up table using a modulo-two summing operation, and each combiner providing a combined data output.

12. A block cipher device according to Claim 1 wherein each second stage further comprises a non-invertible operation unit downstream from said n^{th} power modulo unit and being responsive to an output signal therefrom, said non-invertible operation unit discarding a portion of the output signal from said n^{th} power modulo unit.

13. A communication system comprising:
a block cipher device for converting an input data block into an output data block, said block cipher comprising

a pair of first stages connected in parallel and receiving the input data block and a control data block, each first stage defining a respective data path and comprising

a first unit responsive to the control data block and the input data block, and

a second unit downstream from said first unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said first unit;

a diffuser connected in both of the data paths for mixing data therebetween;

a key scheduler receiving a key data block and generating a random key data block based thereon;

a pair of second stages connected in parallel downstream from said first stages and receiving the random key data block, the control data block and output signals from said first stages, each second stage defining a respective second data path and comprising

a first modulo unit responsive to the random key data block, one of the output signals from said first stages, and the control data block for performing a modulo operation based on a first modulus q,

an nth power modulo unit responsive to an output signal from said first modulo unit for performing an nth power modulo operation based on a second modulus p, and

a second modulo unit responsive to the random key data block and an output signal from said n^{th} power modulo unit for performing a

27

modulo operation based on a third
modulus r,

each first, second and
third modulus q, p and r being unique
from each other; and
an output stage connected to said
second stages for generating an output data
block for said block cipher device.

14. A communication system according to Claim
13 wherein said first unit comprises a sum modulo-two
unit, said second unit comprises a nibble swap unit, and
said first and second modulo units comprise first and
second linear modulo units for performing summing
operations.

15. A communication system according to Claim
13 wherein said block cipher device operates as an
encrypter.

16. A communication system according to Claim
13 wherein said block cipher device operates as a
decrypter.

17. A communication system according to Claim
13 further comprising circuitry connected to said block
cipher device so that said block cipher device operates
in at least one of a block cipher feedback mode, a
minimum error propagation mode and a self-synchronizing
feedback mode.

18.   A communication system according to Claim 13 wherein said first and second stages are selectively configurable so that one first data path and one second data path are operational; and wherein said diffuser is bypassed.

19.   A communication system according to Claim 13 wherein said diffuser is connected in both of the first data paths between the respective first and second units.

20.   A communication system according to Claim 13 wherein each first stage further comprises a substitution/expansion unit downstream from said second unit and being responsive to an output signal therefrom for providing customizable cipher variations.

21.   A communication system according to Claim 20 wherein each first stage further comprises a second nibble swap unit downstream from said substitution/ expansion unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said substitution/expansion unit.

22.   A communication system according to Claim 13 further comprising a nibble interleave unit connected in both of the first data paths for reordering data therebetween.

23.   A communication system according to Claim 13 further comprising a substitution unit connected in

both of the first data paths for substituting data
therebetween.

24. A communication system according to Claim
13 wherein each nth power modulo unit provides an output
signal of predetermined size, with n>1 and with $p=2^K-X$,
where X is selected such that a greatest common
denominator between n and (2^K-X-1) is 1 and K is the
predetermined size.

25. A communication system according to Claim
13 wherein said key scheduler comprises a pair of look-up
tables for generating the random key data block.

26. A communication system according to Claim
25 wherein said key scheduler further comprises a pair of
shift registers responsive to the received key data
block; and wherein each look-up table is responsive to a
corresponding shift register.

27. A communication system according to Claim
26 wherein said key scheduler comprises a pair of
combiners responsive to outputs from said shift registers
and to outputs from said look-up tables, each combiner
combining the output from a corresponding shift register
and the output from a corresponding look-up table using a
modulo-two summing operation, and each combiner providing
a combined data output.

28. A communication system according to Claim
13 wherein each second stage further comprises a non-
invertible operation unit downstream from said n^{th} power

modulo unit and being responsive to an output signal therefrom, said non-invertible operation unit discarding a portion of the output signal from said n^{th} power modulo unit.

29. A method for converting an input data block into an output data block for a cryptographically secured digital communication system, the method comprising:

providing the input data block, a control data block and a random key data block to parallel data paths in the digital communication system;

combining the control data block and the input data block within each data path to provide a first data output signal for each data path;

transposing segments of the first data output signal within each data path in response to the control data block to provide a second data output signal within each data path;

mixing data between the parallel data paths;

performing a first linear modulo operation based on a modulus q within each data path in response to the second data output signal, the random key data block and the control data block to provide a third data output signal within each data path;

performing an nth power modulo operation based on a second modulus p within each respective data path in response to the third data output signal to provide a fourth data output signal within each data path; and

performing a second linear modulo operation based on a third modulus r within each respective data path in response to the random key data block and the

fourth data output signal to provide an output data block, each first, second and third modulus q, p and r being unique from each other.

30. A method according to Claim 29 wherein the cryptographically secured digital communication system is selectively configurable so that one data path is operational.

31. A method according to Claim 29 further comprising performing a substitution/expansion operation within each data path on the second data output signal to provide customizable cipher variations.

32. A method according to Claim 31 further comprising performing a nibble swap operation within each data path on the customizable cipher variations in response to the control data block for reordering the customizable cipher variations.

33. A method according to Claim 32 further comprising performing a nibble interleave operation for reordering data between the data paths for the reordered customizable cipher variations.

34. A method according to Claim 33 further comprising performing a substitution operation after the nibble interleave operation for substituting the reordered customizable cipher variations between the parallel data paths.

35. A method according to Claim 29 wherein each nth power modulo operation provides an output signal of predetermined size, with n>1 and with $p=2^K-X$, where X is selected such that a greatest common denominator between n and (2^K-X-1) is 1 and K is the predetermined size.

36. A method according to Claim 29 wherein the random key data block is generated by a key scheduler comprising a pair of look-up tables.

37. A method according to Claim 36 wherein the key scheduler further comprises a respective shift register associated with each look-up table.

38. A method according to Claim 37 wherein the key scheduler further comprises a pair of combiners responsive to outputs from the shift registers and to outputs from the look-up tables, each combiner combining the output from a corresponding shift register and the output from a corresponding look-up table using a modulo-two summing operation, and each combiner providing a combined data output.